Powerful Privacy Potential:

P3P in the Context of Legislation and Education

Charlin Lu

Professor Feigenbaum

Sensitive Information in a Wired World

December 14, 2003

Increasing Personal Data Collection with Little Consumer Control

In the past two decades, the Internet has gone from being the exclusive domain of scientific and academic researchers to a medium central to mainstream life. The general public now chats online, orders groceries online, checks the weather online, purchases plane tickets online, reads the news online, and much more. With the growing commercialization of the Internet and the increasing sophistication of computer technology, more and more websites have begun gathering information about their visitors, creating profiles and storing data based on their registration information, as well as their browsing and shopping habits.[1] The vast proliferation of personal information being collected, along with consumers' inability to know what is being gathered and how to prevent it, has resulted in mounting consumer anxiety over the degree to which their online activities are being monitored and their privacy invaded. Harris public opinion polls revealed that privacy concerns are the number one reason that people choose to stay off the Internet,[2] and Westin found that 81% of Internet users are concerned about their privacy while online.[3] This widespread discomfort has translated into difficulties for the development of web-based commerce. As described by Scott Cooper and Barbara Lawler, Manager and Chief Privacy Officer of Hewlett-Packard, "If the ability to spend is the fuel that propels the economic engine, then consumers' trust and confidence in that engine is the lubricant."[4]

Not only do these feelings of mistrust impede the expansion of e-commerce, they reflect the degree to which such aggregation of personal information intrudes upon individual privacy. Most people would agree that privacy entails the ability to control the disclosure and subsequent use of personal information.[5] One of the main problems with the online collection of personal data is that Internet users are not given the chance to either consent or refuse to share their

personal information. Consent is widely recognized as fundamental to an individual's ability to protect his or her privacy, both as a principle of the Fair Information Practices[6] and as a central tenet of the Organization for Economic Cooperation and Development (OECD)'s Guidelines for the Protection of Data and Transborder Data Flows.[7] Naturally, unless a web site notifies its visitors exactly what information is being collected and what it will be used for, it is impossible for the visitor to make an informed choice about whether he or she wishes to reveal this information. Consequently, notice is a necessary prerequisite for consent.

While many websites have privacy policies, they tend to be difficult and time-consuming to locate, to read, and to understand. Moreover, they may change frequently without notice. It is unreasonable to expect Internet users to carefully read the privacy policy of every website they visit each time they visit, and in reality, many people do not take the time to read a site's privacy policy even on their initial visit. A study by the Privacy Leadership Initiative found that 31% of the public spends little or no time reading online privacy policies.[8] While an overwhelming majority of consumers want a short privacy notice with a common format to facilitate comparison, what most websites have are long privacy policies filled with legal jargon, difficult to understand, much less to compare across organizations.[9]

Development and Design of P3P

In response to escalating privacy concerns, the World Wide Web Consortium (W3C) sought to create a standard and convenient way for web sites to communicate their privacy policies to visitors. (The purpose of W3C, an international, nonprofit, industry-supported consortium, is to guide the Web's development while considering the legal, social, and commercial implications of its technology.) In 1997, W3C embarked on the project of designing the Platform for Privacy Preferences (P3P), a standard, computer-readable format for privacy

policies and a protocol allowing user agents such as web browsers to read and process these policies automatically. Participants in this project included representatives from around the world in industry, government, nonprofit organizations, and academia.[10] After years of effort, W3C released P3P specification 1.0 in April of 2002.

For P3P to work correctly, users must indicate their privacy preferences, and websites must express their privacy policies according to the P3P specification. With a P3P-enabled user agent, which can be any software tool used to access the Internet, the user may express his or her privacy preferences, whether by adjusting a privacy slider, answering a series of multiple choice questions, or checking off items on a list. To some degree, the granularity with which a user may manipulate his or her privacy preferences depends on the sophistication of the user agent. Some currently available user agents include Microsoft's Internet Explorer 6.0, Netscape Navigator 7, and AT&T's Privacy Bird, with the Privacy Bird providing the most functionality in terms of P3P.

On the side of the website, P3P privacy policies are written in Extensible Markup Language (XML) and answer the following questions: 1) Who is collecting this data? 2) Exactly what information is being collected? 3) For what purpose? 4) Which information is being shared with others? 5) And who are these data recipients? 6) Can users access their own data? 7) Can users make changes in how their data is used? 8) How are disputes resolved? 9) What is the policy for retaining data? 10) Where can the detailed policies be found in "human readable" format?

When a user wishes to view a website that has been P3P-enabled, either with one policy for the entire site or varying policies for different sections of the site, the user agent automatically requests the site's P3P policy, using HyperText Transfer Protocol (HTTP). Then

the user agent compares the site's privacy policy with the user's privacy preferences and acts accordingly. If the site's privacy policy violates the user's privacy preferences, there may be a noise or symbol warning of the mismatch and a message explaining the difference between the site's policy and the user's selection of privacy preferences so that the user can make an informed choice about whether he or she wishes to proceed. Otherwise, the user is allowed to enter the site without interruption, though a symbol may be displayed or a noise sounded to indicate that the site's privacy policy has been approved. In addition, user agents generally provide a toolbar icon that the user can click on to see a simple and standardized version of the site's privacy policy in human readable form.

Advantages and Shortcomings of P3P

P3P makes privacy notices easy to locate and to understand, cutting through the legalese and providing a consistent format so that they can be compared across sites. The protocol allows users to specify their privacy preferences once so that they can be automatically compared to a website's privacy policy each time the site is visited. With this clarity and ease of use, P3P promotes transparency and thus increases accountability on the part of the website owner. Additionally, through symbols, sounds, and warning messages, P3P user agents provide information to assist individuals in making decisions about when to disclose personal information, how much, and to whom. P3P provides for a system of notice and consent by providing information about what information is being gathered and how it will be used so that users can assess the risks and benefits of disclosure before making an informed choice.

P3P works in a sensible and intuitive manner. For a user to exercise control over his or her personal information, notice should be delivered whenever personally identifiable information is about to be collected. Yet at the same time, both users and website owners would

like to maintain a seamless browsing experience to the greatest extent possible.[11] P3P interrupts the user's browsing only when necessary to inform the user of discrepancies in his stated preferences and the site's policy, so that he or she can then make an informed choice.

The advantages of P3P go beyond the obvious beneficial effects of increased knowledge and transparency. Even the process of making a site P3P-compliant is in itself a worthwhile undertaking. The systematic procedure that a website undergoes in becoming P3P-compliant can help to uncover gaps in existing privacy policies.[12] The process forces the company or organization to scrutinize its privacy policy and become fully aware of its nuances and its practical implications—a necessary prerequisite for the actual implementation of any privacy policy. Moreover, by providing an open standard for expressing privacy policies, P3P makes it possible to accurately and automatically rate and block websites whose privacy policies do not meet certain standards. Accordingly, it both encourages the development of new privacy enhancing products and services and can be helpful in policing compliance for countries that have data protection and privacy laws.[13]

Nonetheless, P3P does have its limitations. Most importantly, it does not include a mechanism for enforcement. It cannot ensure that companies or organizations will actually follow the privacy policies on their websites. Therefore, it does not replace privacy regulations and cannot guarantee privacy protection for websites owned in jurisdictions with insufficient data privacy laws.[14]

Brewing Controversy over P3P

Since its inception, there has been much controversy over P3P. It has both been "lauded as the answer to everyone's privacy worries and castigated as a Trojan horse that will divert public attention away from real problems."[15] Professor Lawrence Lessig of Stanford Law

School, an enthusiastic supporter of P3P, has hailed it as "the most promising solution to cyberspace privacy." Likewise, Christine Varney, former FTC Commissioner, commended it as a means for helping "responsible online business empower users to choose the privacy relationship best for them."[16] On the other hand, opponents of P3P have denigrated it as "Pretty Poor Privacy"[17] or a "Pretext for Privacy Procrastination."[18]

The main issue dividing supporters and opponents of P3P is their view on where the real problem with online data collection lies. Opponents perceive the gathering of data itself as the problem, while supporters believe users' inability to make an informed choice due to their lack of knowledge about the nature and purpose of the information gathered is the problem.[19] Because opponents of P3P believe personal data collection is neither necessary nor beneficial to consumers, they propose psuedonymity or anonymity as far better solutions since they minimize or completely eliminate the collection of personally identifiable information. In their eyes, P3P is little more than a "tacit acceptance of the great increase in the tracking and monitoring of our minor activities that take place over the Web."[20]

The underlying assumption beneath this view is that consumers never benefit from sharing their personal information, and thus there is no need for a mechanism allowing individual choice. However, evidence from other commercial realms suggest otherwise. Just as most people find that the convenience of using a credit card outweighs the disadvantage of having one's purchases tracked and recorded, many people may be willing to give up varying amounts of personal information in exchange for desired benefits, such as site customization, not having to retype billing and shipping information, receiving purchase recommendations, or entering into a sweepstake for a car or a vacation. P3P allows individuals to make their own

informed decisions about when to disclose personal information rather than assuming a shared privacy standard for people from all over the world.

Because privacy protection on the Internet is a global problem, it needs a solution that is flexible, both to accommodate users of various social, economic, and cultural backgrounds and to work effectively across national borders.[21] Regardless of whether consumers do or do not have a diverse range of privacy preferences, even the strictest privacy laws cannot be enforced beyond a country's national jurisdiction. Technological standards such as P3P, however, can allow citizens of any nation to make an informed choice about whether or not to enter a site that may or may not abide by their country's privacy standards. The designers of P3P recognized that a descriptive standard provides more flexibility and thus is more useful internationally than a normative system. Accordingly, they intentionally created P3P as a mechanism rather than as a policy.[22] By providing a mechanism for expressing privacy practices, they left policy decisions in the hands of individual users and/or national legislatures.

Beyond their differing views on the need for data collection and for personal choice, there is actually far less disagreement than it may first seem between the two camps. Both supporters and opponents of P3P recognize that P3P lacks an enforcement mechanism; however, critics do not seem to realize that even the strongest advocates for P3P acknowledge this limitation. Opponents seem to fear that P3P can or will be used only in conjunction with self-regulation. Accordingly, much of their criticism stems from the belief that P3P precludes the possibility of any meaningful privacy legislation. Yet proponents of P3P have clearly recognized that P3P is meant to complement laws, technology tools, and privacy seal programs, not to replace them. In fact, W3C, the creator of P3P, has unequivocally declared, ""P3P does not protect privacy, in and of itself. It does, however, help create a framework for informed choice

on the part of consumers. Any efficacy that P3P has is dependent upon the substantive privacy rules established through other processes – be they a result of regulatory, self-regulatory, or public pressure."[23] Supporters of P3P generally acknowledge that notice alone does not ensure that an organization abides by its policy but see the provision of notice, the "lynchpin of the fair information practices,"[24] as a step in the right direction. Just as most declarations of praise for P3P are tempered with recognition of its limitations, a closer look at the evidence critics cite in their condemnation of P3P reveals that their censure of P3P is largely conditioned on the lack of a regulatory framework. For example, one of the much-quoted statements made by the European Commission, often put forth as evidence of the EU's rejection of P3P, merely says, "A technical platform for privacy protection…must be applied within the context of a framework of enforceable data protection rules, which provide a minimum and non-negotiable level of privacy protection for all individuals. Use of P3P *in the absence of such a framework* risks shifting the onus primarily onto the individual user to protect himself" (emphasis added).[25]

As it turns out, supporters and opponents of P3P have more in common than one might think at first glance. If they would work together to advocate a solution in a united voice rather than confusing the public with their contentious cacophony, Internet users could reap the benefit of their privacy expertise. Most of the existing criticism aimed toward P3P either assumes that P3P precludes privacy legislation or addresses an issue due to lack of user education rather than an inherent fault in P3P. The answer is to use P3P in concert with legislation and education.

Need for Legislation and Education

Before P3P can reach its full potential as a technological tool for the advancement of privacy protection, it needs an enforcement mechanism to ensure that the privacy policies it expresses are reflected in actual practice.[26] Arguably, privacy legislation is the best way to

provide this enforcement. In a May 2000 report to Congress entitled "Privacy Online: Fair Information Practices in the Electronic Marketplace," the Federal Trade Commission (FTC) recommended enacting privacy legislation because "self regulatory programs alone cannot ensure that the online marketplace as a whole will emulate the standards adopted by industry leaders."[27] This is not to say that market pressure and self-regulatory programs such as voluntary privacy seal programs have no place in the use of P3P. Rather the FTC merely recognizes the fact that only legislation can guarantee consumers a minimum standard for privacy protection across the board. P3P can and should be applied in the context of privacy legislation, serving to complement rather than to substitute privacy regulations. For example, P3P contains mechanisms which support some of the privacy protection requirements of Germany's Teleservices Data Protection Act (TDDSG) and the Agreement on Media Services of the Federal Länder (MDStV), such as the obligation to inform users before collection about type, scope, and purpose for collecting personal data and to notify users about policies for forwarding of data and procedures for dispute resolution.[28]

In many respects, P3P is similar to food and drug labeling – it provides information in a standard, easily understood format so that consumers can make their own choices. Just like labels, P3P policies are not particularly useful without the guarantee that the information stated in an organization's policy reflects its actual business practices. Consumer protection laws that prevent and punish false advertising and deceptive trade practices could be extended to explicitly include P3P policies, or legislation could be enacted that defines P3P policies as legally binding contracts. Either method would resolve the current situation of legal uncertainty around P3P policies (as well as website privacy policies in general) and would serve as a means for enforcement.[29]

Additionally, governments that do not already have adequate privacy protection standards should mandate a general privacy baseline. In many other areas, such as food, drugs, and the environment, governments require corporations to meet a minimum standard, while allowing market competition to determine the rest.[30] Governments can issue a privacy seal of approval much like FDA approval to sites whose privacy practices have been audited and have met the baseline standard. Though any national government can only enforce its privacy protection laws within its own jurisdiction, P3P user agents could check the website owner's geographical location and its dispute resolution clause in order to ensure that users only enter sites bound by certain national privacy laws or that a warning is shown before entering any site that is not bound by these laws.

A permanent privacy agency should be created to ensure that privacy protection laws are in enforced. Just as the Food and Drug Administration (FDA) is necessary for effective consumer protection, "the cornerstone of an effective federal [privacy] policy is a permanent privacy agency."[31] A privacy agency can provide guidance for future recommendations on issues concerning privacy protection. Additionally, having a government office with the expertise and authority to advocate on privacy matters ensures that whenever the government seeks to expand its monitoring and surveillance activities, national security and law enforcement needs will be balanced against citizens' privacy interests.

Enacting privacy legislation would solve many of the shortcomings associated with P3P. One of problems faced by P3P is that it has not been widely adopted. As of July 2003, only 30% of the top 100 and 21% of the top 500 websites were P3P-compliant.[32] However, if P3P policies were either mandated or offered as a possible compliance option for websites, P3P adoption would increase rapidly.[33] Once more sites have become P3P-compliant, new P3P tools that

make it easier to for users to identify privacy-friendly sites, such as P3P-enabled search engines or comparison-shopping services, are also likely to develop, further motivating websites to adopt privacy-friendly practices.[34]

Another oft-cited deficiency of P3P is that it fails to provide actual choice. According to opponents, because many sites have revenue models supported by advertising, privacy-conscious users who configure their privacy preferences to have high privacy protections will face endless pop-up windows warning them that sites do not meet their privacy preferences. As a result, they will be forced to lower their privacy preferences in order to browse most of the Internet, thus maintaining the privacy invasive status quo.[35] What these critics fail to recognize is that even in this worst-case scenario, users will become more aware of just how much of their personal information is being collected and have the chance to choose whether they really want to use the online service or not. Secondly, increased transparency and heightened public awareness of privacy invasive policies may cause companies to change their privacy policies. Finally, regardless of the success or failure of consumer pressure, national privacy legislation can force websites located within its jurisdiction to maintain a baseline level of privacy protection. Once such legislation is in place, P3P is a helpful and convenient tool for users to distinguish between those sites that are required to follow their national privacy standards and sites (outside of federal jurisdiction) that are not, as well as to identify sites that voluntarily go beyond the minimum privacy requirements.

Yet another common complaint that would be remedied with privacy legislation is the claim that P3P places the burden on individual users to protect their rights, rather than on the data controller. Critics argue that if users must take additional steps to safeguard their privacy, most people will not take those steps, and the result will be a lack of privacy protection for the

general public.[36] In particular, studies have demonstrated that Internet users find changing default cookie settings to be burdensome and confusing.[37] Hence, it is likely that the default privacy preference settings on a P3P user agent would amount to the degree of privacy protection that P3P would provide most users. This line of reasoning assumes that P3P can only act as a substitute for privacy legislation rather than as a technological tool that aids and complements privacy laws. Certainly, P3P user agents should be made as simple and user-friendly as possible, but by enacting privacy legislation, governments can also provide a minimum level of protection for all sites within their jurisdiction, regardless of users' P3P privacy preferences. Opponents seem to overlook the fact that, short of censoring the Internet so that citizens in a country can only view sites that are within that country's jurisdiction, individual users will always be forced to make some of their own decisions. This hearkens back to the earlier discussion about the need for individual choice when dealing with a global medium like the Internet. A standard like P3P enables users to make this choice in the most informed way possible. Furthermore, P3P has been designed so that governments, privacy advocacy groups, and other trusted organizations can create their own recommended settings for privacy preferences such that an unsophisticated user can import those settings onto his or her user agent with just a few clicks of the mouse.[38] As a last resort, if truly necessary, governments could even require P3P user agent software sold within its national borders to set the default in accordance with federal baseline standards.

Some opponents contend that P3P will result in greater consumer and business confusion over privacy rights and responsibilities, citing the European Commission's declaration that there is a "risk that P3P…could mislead EU-based operators into believing that they can be discharged of certain of their legal obligations…if the individual user consents into this…P3P might thus cause confusion not only among operators as to their obligations, but also among Internet users

as to the nature of their data protection rights."[39] Undeniably, few people are willing to invest much time to protect their own privacy, and many do not understand the extent to which their data is collected or what privacy rights they have, much less the nature of P3P.[40] However, temporarily bypassing this issue and lambasting any technology that requires a modicum of user involvement will only make the problem fester over time. User education is necessary to address the root of the problem. As a first step, P3P translates privacy policies written with legal terminology into an easily understood, standardized format, helping users understand what information is being collected and why. Privacy education campaigns can further spread awareness about the rights of users, the obligations of data controllers, and the role of P3P and other technological tools in the protection of personal information.

Similarly, education is the key to alleviating worries that P3P will be detrimental to Internet privacy because it can and will be used by companies lobbying for self-regulation as a procrastination tool to prevent the passage of meaningful privacy legislation.[41] Regardless of whether companies such as Microsoft, that have helped to develop P3P, did so with ulterior motives in mind, there is no reason to assume that legislators are incapable of understanding the concept espoused by supporters and opponents alike: P3P is useful only in the context of an enforcement mechanism. Rather than fulminating against P3P, the Electronic Privacy Information Center and Junkbusters could spend their time and energy explaining to legislators (and to the general public) why P3P must be used in a legislative context to be effective. Whether lobbying legislators or embarking on a full-fledged public advertising campaign, the end result—heightened awareness, both of Internet privacy as an issue in general and of the advantages and limitations of P3P—would benefit users and could result in privacy legislation.

At the same time, privacy legislation does not preclude additional self-regulatory programs. Rather, by increasing awareness and adoption of P3P, it encourages the development of privacy seals programs, rating services, and privacy auditing firms. When combined with verification by independent auditing firms, P3P increases both transparency and accountability, giving companies more incentives to adopt privacy-friendly practices. While privacy legislation is needed to provide a minimum level of protection, market forces may result in some companies voluntarily implementing privacy policies that go beyond the baseline requirements as a show of their corporate responsibility and respect for customers' privacy. Several studies have shown that consumer trust can make a significant difference in e-commerce. An e-commerce trust study reported that "enhancing the perceived trustworthiness of a site significantly enhances the ability of a site to compete,"[42] and a Harris Interactive Survey found that consumers would do more business with companies that proved they actually carried out their privacy policies in their business practices.[43] Proof of privacy practices requires more than what most privacy seal programs offer today. Whereas existing privacy seals generally reflect little more than an organization's self-assertion of compliance with its stated privacy policy, earning an assurance report through robust testing and verification by an independent auditing firm can provide consumers with a higher level of confidence that is warranted.

Another motivating factor for companies or organizations to adopt privacy-friendly policies beyond the minimum requirement is their desire to improve the accuracy of the information that they collect.[44] Providing the purpose and scope of data collection through a P3P policy and proving compliance with an assurance report can improve the quality of information gathered without too much of a decrease in quantity.[45] In public opinion surveys, the top reason listed by respondents for not filling out online registration forms at sites was "information is not

provided on how the data is going to be used," and Hine and Eve found that much of the discomfort with the Internet today results from not knowing or not trusting the information practices of websites: "in the absence of straightforward explanations on the purposes of data collection, people were able to produce their own versions of the organization's motivations that were unlikely to be favorable. Clear and readily available explanations might alleviate some of the unfavorable speculation."[46] Thus, service providers seeking to gather accurate data on their customers have an incentive to increase their customers' confidence through P3P policies and independent verification.

Conclusion

P3P is neither a cure-all panacea nor a wasted effort. On one hand, it provides users with convenience and increases transparency; on the other, supporters and opponents alike realize that P3P desperately needs a means of enforcement. When combined with privacy regulations and user education, it has the potential to protect and empower users as a means for informed choice. Many Internet users do not realize the degree to which their personal information is gathered, nor do they understand how to prevent such data collection. Only public education campaigns can combat this lack of awareness, and only privacy legislation can guarantee a minimum level of privacy protection. Not only would user education and privacy legislation address many of the concerns critics have about P3P, these efforts would increase both awareness and adoption of a protocol that is comprehensive enough for the implementation of national baseline standards and flexible enough for global use. Once consumers, businesses, and legislators fully comprehend the advantages and limitations of P3P, this promising tool may finally be used to its fullest potential.

References

[1] Daniel J. Weitzner, "Before the United States Senate Committee on Commerce, Science, and Transportation," 25 Mar. 2000.
[2] Marc Rotenberg, "Testimony and Statement for the Record of Marc Rotenberg on Communications Privacy before the Subcommittee on Courts and Intellectual Property, House Judiciary Committee, U.S. House of Representatives," 26 Mar. 1998.
[3] Mark S. Ackerman, Lorrie Faith Cranor, and Joseph Reagle, "Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences," *ACM Conference on Electronic Commerce* (1999): 1-8, online, Internet, 10 Oct. 2003.
[4] Barbara Lawler and Scott Cooper, "The Opt-In Approach to Choice," *Considering Consumer Privacy: A Resource for Policymakers and Practitioners*, ed. Paula J. Bruening (Center for Democracy and Technology, 2003): 22-23, online, Internet, 25 Oct. 2003.
[5] Mary J. Culnan, "How Privacy Notices Promote Informed Consumer Choice," *Considering Consumer Privacy: A Resource for Policymakers and Practitioners*, ed. Paula J. Bruening (Center for Democracy and Technology, 2003): 12-16, online, Internet, 25 Oct. 2003.
[6] "The Code of Fair Information Practices," *Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens* (U.S. Department of Health, Education, and Welfare, 1973), online, Internet, 10 Nov. 2003.
[7] "The OECD Principles," *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (Paris: OECD, 1980), online, Internet, 10 Nov. 2003.
[8] Culnan 12-16.
[9] "P3P 1.0: A New Standard in Online Privacy" (W3C, 1997), online, Internet, 10 Oct. 2003.
[10] Lorrie Faith Cranor, *Web Privacy with P3P* (Beijing: O'Reilly, 2002) 3-11.
[11] Patricia Faley, "Notice," *Considering Consumer Privacy: A Resource for Policymakers and Practitioners*, ed. Paula J. Bruening (Center for Democracy and Technology, 2003): 17-20, online, Internet, 25 Oct. 2003.
[12] Lorrie Faith Cranor, "The Role of Privacy Enhancing Technologies," *Considering Consumer Privacy: A Resource for Policymakers and Practitioners*, ed. Paula J. Bruening (Center for Democracy and Technology, 2003): 80-83, online, Internet, 15 Oct. 2003.
[13] Deirdre Mulligan, Ari Schwartz, Ann Cavoukian, and Michael Gurski, *P3P and Privacy: An Update for the Privacy Community* (Center for Democracy and Technology, 2001), online, Internet, 19 Oct. 2003.
[14] Rüdiger Grimm and Alexander Rossnagel, "Can P3P Help to Protect Privacy Worldwide?" (ACM, 2003), online, Internet, 20 Nov. 2003.
[15] Simson Garfinkel, "Can a Labeling System Protect Your Privacy?" *Salon.com* (Salon Media, 2000), online, Internet, 10 Nov. 2003.
[16] "P3P 1.0: A New Standard in Online Privacy."
[17] Karen Coyle, *P3P: Pretty Poor Privacy? A Social Analysis of the Platform for Privacy Preferences* (Karen Coyle, 1999), online, Internet, 19 Oct. 2003.
[18] Jason Catlett, "Open Letter 9/13 to P3P Developers" (Junkbusters, 1999), online, Internet, 15 Oct. 2003.
[19] Priscilla Regan, "The Role of Consent in Information Privacy Protection," *Considering Consumer Privacy: A Resource for Policymakers and Practitioners*, ed. Paula J. Bruening (Center for Democracy and Technology, 2003): 24-27, online, Internet, 25 Oct. 2003.
[20] Karen Coyle, *A Response to "P3P and Privacy: An Update for the Privacy Community"* (Center for Democracy and Technology, 2000), online, Internet, 19 Oct. 2003.
[21] Ackerman, Cranor, and Reagle 1-8.
[22] Lorrie Faith Cranor and Joseph Reagle, "Designing a Social Protocol: Lessons Learned from the Platform for Privacy Preferences Project," *Proceedings of the Telecommunications Policy Research Conference* (Alexandria, Virginia: 1997), online, Internet, 19 Oct. 2003.
[23] Mulligan, Schwartz, Cavoukian, and Gurski
[24] Culnan 12-16.
[25] James A. Harvey and Karen M. Sanzaro, "P3P and IE6: Raising More Privacy Issues Than They Resolve?" *GigaLaw.com* (Dolesco, 2000), online, Internet, 19 Oct. 2003.
[26] Rotenberg.

[27] Jerry DeVault, Brian Tretick, and Kevin Ogorzelec, "Privacy and Independent Verification: What Consumers Want," *Considering Consumer Privacy: A Resource for Policymakers and Practitioners*, ed. Paula J. Bruening (Center for Democracy and Technology, 2003): 100-102, online, Internet, 25 Oct. 2003.
[28] Grimm and Rossnagel.
[29] Harvey and Sanzaro.
[30] Garfinkel.
[31] Rotenberg.
[32] *P3P Dashboard Report: July 2003* (Ernst & Young LLP, 2003), online, Internet, 10 Oct. 2003.
[33] Cranor, "The Role of Privacy Enhancing Technologies" 80-83.
[34] Lorrie Faith Cranor and Rigo Wenning, "Why P3P is a Good Privacy Tool for Consumers and Companies," *GigaLaw.com* (Dolesco, 2000), online, Internet, 19 Oct. 2003.
[35] Electronic Privacy Information Center and Junkbusters, *Pretty Poor Privacy: An Assessment of P3P and Internet Privacy*, (2000), online, Electronic Privacy Information Center, Internet, 19 Oct. 2003.
[36] Regan 24-27.
[37] Electronic Privacy Information Center and Junkbusters.
[38] Cranor and Reagle
[39] Electronic Privacy Information Center and Junkbusters.
[40] Ackerman, Cranor, and Reagle 1-8.
[41] Catlett.
[42] Stephen Marsh, John F. Meech, and Ala'a Dabbour, "Putting Trust into E-commerce – One Page at a Time," *Proceedings of the Fourth International Conference on Autonomous Agents* (Barcelona: National Research Council of Canada, 2000): 73-80, online, Internet, 10 Oct. 2003.
[43] DeVault, Tretick, and Ogorzelec 100-102.
[44] Grimm and Rossnagel.
[45] Lawler and Cooper 22-23.
[46] Ackerman, Cranor, and Reagle 1- 8.